PATENT ABSTRACTS OF JAPAN

2

(11)Publication number : 2000-244655
(43)Date of publication of application : 08.09.2000

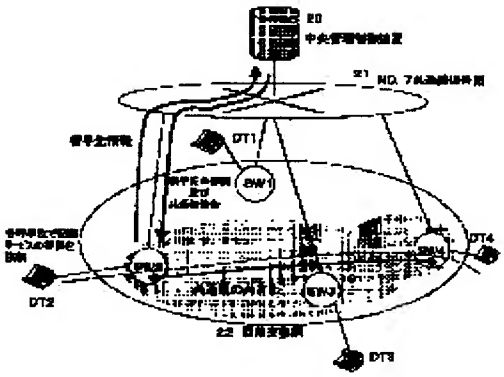
(51)Int.Cl. H04M 3/42
G06F 13/00
H04L 9/08
H04L 12/66
H04M 3/00
H04M 7/00

(21)Application number : 11-039995
(22)Date of filing : 18.02.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : KIMURA MISAO

(54) NETWORK SYSTEM HAVING SECRECY SERVICE FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a network system having a secrecy service function by which unitary key management is executed by enciphering the open key of a call opposite party exchange and a common key for enciphering a message whenever a call requesting secrecy communication occurs and distributing them.
SOLUTION: A central management controller 20 and respective exchanges distribute the keys on demand by constituting a network independent of the public line network 22. For example, the exchange SW2 transmits opposite party information to the controller 20 when a call is made. The controller 20 transmits opposite open key and common key information to the exchange SW2 by retrieving a database. The exchange SW2 enciphers common key information by the opposite party open key and transmits it to the exchange SW4 of the opposite party. The common key is obtained by decoding through the use of one's own open key. Therefore, message information is exchanged between the exchanges SW2 and SW4 by enciphering it by using the common key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－244655
（P2000－244655A）
(43)公開日　平成12年９月８日(2000.9.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｍ　3/42		Ｈ０４Ｍ　3/42	Ｚ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｍ　3/00	Ｄ	５Ｋ０２４
12/66		7/00	Ｚ	５Ｋ０３０
Ｈ０４Ｍ　3/00		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｋ０５１

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－39995

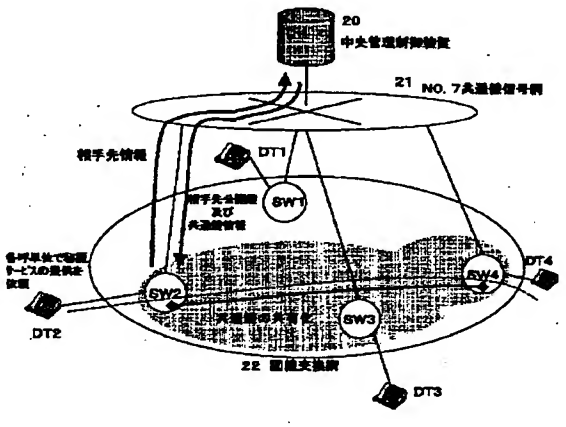
(22)出願日　平成11年２月18日(1999.2.18)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　木村　操
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100094514
弁理士　林　恒徳　（外１名）

最終頁に続く

(54)【発明の名称】　秘匿サービス機能を有するネットワークシステム

(57)【要約】
【課題】中央管理制御装置を備え、一元的に鍵管理を実施することが可能とする秘匿サービス機能を有するネットワークシステムを提供する。
【解決手段】それぞれ暗号化部を有する中央管理制御装置と複数の交換機を有して構成され、中央管理制御装置は、通話相手先交換機の公開鍵と、メッセージ通信を行なう交換機間で送受されるメッセージを暗号化するための共通鍵を、秘匿通信を要求する呼の発生の都度、呼の発生を検出する交換機に対し、暗号化部で暗号化して配信する。前記中央管理制御装置は、前記複数の交換機の公開鍵をデータベースとして保持し、前記呼の発生した交換機から相手先ダイヤル番号と自交換機の利用者番号を通知され、通知された相手先ダイヤル番号と自交換機の利用者番号を基に、該データベースから相手先ダイヤル番号を収容する相手先交換機の公開鍵を検索し、相手先交換機の公開鍵と呼の発生を検知する交換機の公開鍵から前記共通鍵を生成する。



【特許請求の範囲】
【請求項１】それぞれ暗号化部を有する中央管理制御装置と複数の交換機を有して構成され、
該中央管理制御装置は、通話相手先交換機の公開鍵と、メッセージ通信を行なう交換機間で送受されるメッセージを暗号化するための共通鍵を、秘匿通信を要求する呼の発生の都度、該呼の発生を検出する交換機に対し、該暗号化部で暗号化して配信することを特徴とする秘匿サービス機能を有するネットワークシステム。
【請求項２】請求項１において、
前記中央管理制御装置は、前記複数の交換機の公開鍵をデータベースとして保持し、
前記呼の発生した交換機から相手先ダイヤル番号と自交換機の利用者番号を通知され、該通知された相手先ダイヤル番号と自交換機の利用者番号を基に、該データベースから該相手先ダイヤル番号を収容する相手先交換機の公開鍵を検索し、該相手先交換機の公開鍵と該呼の発生を検知する交換機の公開鍵から前記共通鍵を生成することを特徴とする秘匿サービス機能を有するネットワークシステム。
【請求項３】請求項１において、
前記呼の発生を検出した交換機は、前記中央管理制御装置から配信される公開鍵を、前記通話相手先交換機の公開鍵で暗号化し、前記通話相手先交換機に送信し、
該通話相手先交換機は、送信された暗号化公開鍵を自交換機の秘密鍵で復号することを特徴とする秘匿サービス機能を有するネットワークシステム。
【請求項４】請求項１において、
前記呼の発生を検出する交換機は、呼の発生の都度、秘匿通信モードに移行する様に制御することを特徴とする秘匿サービス機能を有するネットワークシステム。
【請求項５】請求項１において、
前記呼の発生を検出する交換機は、呼の情報から秘匿通信モードに移行する指示を検出することにより、秘匿通信モードに移行する様に制御することを特徴とする秘匿サービス機能を有するネットワークシステム。
【請求項６】それぞれ暗号化部を有する中央管理制御装置と複数の交換機を有して構成されるネットワークシステムにおける秘匿通信のための暗号化鍵の配信方法であって、
呼の発生を検出する交換機から相手先ダイヤル番号と自交換機の利用者番号を該中央管理制御装置に通知し、
該中央管理制御装置は、データベースから該相手先ダイヤル番号に基づき相手交換機の公開鍵を検索し、且つ該検索された相手交換機の公開鍵と該呼の発生を検出する交換機の公開鍵から共通鍵を生成し、
該該呼の発生を検出する交換機は、該検索された相手交換機の公開鍵で該生成された共通鍵を暗号化し、且つ該相手交換機に送り、
該相手交換機は、自交換機の秘密鍵で該送られた共通鍵を再生することを特徴とする秘匿サービス機能を有する秘匿サービス機能を有するネットワークシステムにおける暗号化鍵の配信方法。
【請求項７】請求項６において、
前記呼の発生を検出する交換機から相手先ダイヤル番号と自交換機の利用者番号の前記中央管理制御装置への通知は、該中央管理制御装置の公開鍵を用いて暗号化されることを特徴とするネットワークシステムにおける暗号化鍵の配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、秘匿サービス機能を有するネットワークシステムに関する。特に、センター局（中央管理制御装置）とネットワークを構成する複数の交換機を有し、交換機に暗号化部を設けて呼の接続の都度、暗号鍵を設定して秘匿通信を行なうネットワークシステムに関する。
【０００２】
【従来の技術】情報を送受するためのネットワーク基盤の整備に伴い情報に関するセキュリティの重要性が再認識されている。情報を送受するためのネットワークは、プライベートにおいてもビジネスにおいても時間及び空間の制約を極めて低減する効果があるため日常生活において必須なものとなっている。
【０００３】ここで、情報は発信側の個人の意識により扱い方が異なる。たとえば第三者にとっては重要な内容でも軽んじて扱われる場合が多々ある。特に、企業における社内ネットワーク等のプライベート・ネットワークにおいては通信事業者の回線を借用することになる。
【０００４】このために公共的な場所を介するにも関わらず内線としての接続が基本であるために、盗聴等の不正に対する対策はあまり対策を講じられていないのが現状である。
【０００５】このためにネットワークを介する情報に関しての盗聴、改竄等の不正に対応するべく秘匿通信のためのさまざまな暗号化技術が開発されている。秘匿通信は、図８により概略的に説明できる。
【０００６】すなわち図８において、（I）に示すように送信側T1から受信側T2にデータが送信される場合、データをそのまま（以下平文と言う）送信することを想定する。この場合回線途中T3において盗聴、改竄が容易である。
【０００７】これに対し図８において、（II）に示されるように送信側T1でデータを暗号化鍵（A）で暗号化して送信する。受信側T2では暗号化データを復号化鍵を用いて平文を再生する。したがって、この場合はデータ内容を平文にするための復号化の作業が必要となり、回線途中での盗聴、改竄を非容易とすることが可能である。
【０００８】さらに暗号化の方法として暗号化鍵（A）と復号化鍵（B）が等しいものとする共通鍵暗号方式と

それぞれが異なる場合の公開鍵暗号方式の２種類がある。

【０００９】共通鍵方式は、送受信側T1、T2が共に同一の鍵を用いて暗号化／復号化する方式である。公開鍵暗号方式は、ＲＳＡ暗号方式に代表されるように一方向性関数を用いて基本的には公開鍵により暗号化を行い、秘密鍵により復号化を行なう方式である。

【００１０】共通鍵方式は、高速処理が可能であるためメッセージ本体の暗号化に使用される。一方、公開鍵暗号方式はソフトウェアでの実現が容易であるが、高速な処理には適していない。このため共通鍵方式における鍵配送等に利用される。

【００１１】また暗号鍵をもとに実際に暗号化を行なう方式としてはDESに代表されるブロック暗号とビット単位に乱数を作用させ暗号化を行なうストリーム暗号化の方式がある。

【００１２】システム例として図９に示すように端末側のそれぞれに備えられる秘匿装置１００により相互で暗号化を行なう端末暗号方式と、図１０に示すようにＴＤＭ装置に秘匿装置１００を設け、これにより回線単位に暗号化を実施する回線暗号方式がある。

【００１３】図９に示す端末暗号方式においては、それぞれ通話毎に相手先が異なる場合（当然に送受ともに同様の秘匿装置１００を必要とする）に、一般的には呼が接続された後に秘匿装置間で暗号化鍵（受信側は復号化鍵）を公開鍵暗号方式により送受して共有化する。

【００１４】一方、回線暗号方式においては、図１０に示すように例えばＴＤＭ（多重化）装置１０１相互間など回線が保証される単位（例えば、1.544Mbps単位）で暗号化を実施する方法である。この方式は処理が単純で高速処理が可能なストリーム暗号で実現されている。ただし、回線がクロスコネクトにより構成されている場合、それぞれの回線単位に秘匿装置１００及び、鍵管理が必要である。

【００１５】これまで、上記のような方式を組み合わせて秘匿システムを実現している。かかる秘匿システムの一例を図１１に示す。端末A～端末間Bで呼が接続された後に、端末A側の秘匿装置１００で実際にメッセージを暗号化する共通鍵を生成する（ステップＳ１）。この共通鍵を端末B側に伝送するために端末Bの公開鍵を用いて共通鍵を暗号化して送信する（ステップＳ２）。

【００１６】端末Bは、自己の秘密鍵により受信暗号化データを復号化する（ステップＳ３）。これにより端末A，B共に共通鍵を共有することになる。したがって、この共有する共通鍵により端末Ａ側の秘匿装置１００でメッセージを暗号化し秘匿通信を実現する。

【００１７】

【発明が解決しようとする課題】一方、近年エレクトロニック・コマース及びインタネット等に関する経済活動に関連する分野においては、個人認証、セキュリティのしくみ等を含め強化されている。しかし、いつでもどこでも不特定な相手と秘匿通信が行えるしくみは提供されておらず、このようなシステムの提供が望まれている。

【００１８】また、上記に説明したように従来秘匿通信を行うためには基本的に導入する回線毎にそれぞれ個別に秘匿装置１００を導入することが必要である。さらに、導入した秘匿装置１００だけでいかなる相手とも秘匿通信が可能となるわけではない。このため、相手先が増える度に秘匿装置１００を増設する必要があり経費がかかる。

【００１９】さらに、セキュリティを万全なものとするためには鍵の管理が重要となる。例えば、上記公開鍵方式の場合においては、ユーザが鍵を共有することが必要になる等、鍵管理は煩雑であり、システム的な一元管理が求められる。これにより管理対象が限定されることになる。

【００２０】したがって、本発明は、かかる従来の問題を解決する秘匿サービス機能を有するネットワークシステムを提供することにある。

【００２１】本発明の目的は、特にプライベート・ネットワークにおいて各ユーザが意識することなく秘匿ネットワークを構築することが可能となる秘匿サービス機能を有するネットワークシステムを提供することにある。

【００２２】また本発明の目的は、セキュリティを強化しシステムの変更なしに個別に特定ユーザに対して秘匿通信を設定することが可能となる秘匿サービス機能を有するネットワークシステムを提供することにある。

【００２３】さらに本発明の目的は、中央管理制御装置を備え、一元的に鍵管理を実施することが可能とする秘匿サービス機能を有するネットワークシステムを提供することにある。

【００２４】

【課題を解決するための手段】上記本発明の課題を解決する秘匿サービス機能を有するネットワークシステムは、それぞれ暗号化部を有する中央管理制御装置と複数の交換機を有して構成される。そして、中央管理制御装置は、通話相手先交換機の公開鍵と、メッセージ通信を行なう交換機間で送受されるメッセージを暗号化するための共通鍵を、秘匿通信を要求する呼の発生の都度、呼の発生を検出する交換機に対し、前記暗号化部で暗号化して配信することを特徴とする。

【００２５】一の態様として、前記において、前記中央管理制御装置は、前記複数の交換機の公開鍵をデータベースとして保持し、前記呼の発生した交換機から相手先ダイヤル番号と自交換機の利用者番号を通知され、この通知された相手先ダイヤル番号と自交換機の利用者番号を基に、前記データベースから相手先ダイヤル番号を収容する相手先交換機の公開鍵を検索する。そして、前記相手先交換機の公開鍵と呼の発生を検知する交換機の公開鍵から前記共通鍵を生成することを特徴とする。

【００２６】また、一の態様として、前記呼の発生を検出した交換機は、前記中央管理制御装置から配信される公開鍵を、前記通話相手先交換機の公開鍵で暗号化し、前記通話相手先交換機に送信する。そして、この通話相手先交換機は、送信された暗号化公開鍵を自交換機の秘密鍵で復号することを特徴とする。

【００２７】さらに、一の態様として、前記呼の発生を検出する交換機は、呼の発生の都度、秘匿通信モードに移行する様に制御することを特徴とする。

【００２８】さらにまた、一の態様として、前記呼の発生を検出する交換機は、呼の情報から秘匿通信モードに移行する指示を検出することにより、秘匿通信モードに移行する様に制御することを特徴とする。

【００２９】上記のように鍵の管理、運用を一元化して実施するセンター局にある中央管理制御装置と交換機を共通線ネットワークで個別に接続することにより、鍵の配信を随時可能とする。また、各呼単位にそれぞれ相手先に応じた鍵を配送することにより、暗号化を行うための条件を中央管理制御装置により管理制御可能となる。

【００３０】本発明の更なる特徴は以下に図面を参照して説明する発明の実施の形態から明らかになる。

【００３１】

【発明の実施の形態】以下図面を参照して本発明の実施の形態を説明する。なお、図において同一又は、類似のものには同一の参照番号又は、参照記号を付して説明する。

【００３２】図１は、本発明に従うネットワークシステムにおける秘匿サービス機能の原理を説明する図である。図１において複数の交換機ＳＷ１～ＳＷ４で公衆回線網２２が構成されている。

【００３３】それぞれの交換機ＳＷ１～ＳＷ４には、加入者端末ＤＴが接続されている。さらに、ＮＯ．７共通線信号網等の信号線ネットワーク２１を通して鍵の管理、運用を一元化して実施するセンター局に複数の交換機ＳＷ１～ＳＷ４のそれぞれが個別に接続される。

【００３４】センター局は中央管理制御装置２０を有し、各交換機は秘匿部を有する。そして、中央管理制御装置２０と各交換機は、公衆回線網２２と別ネットワークを構成することにより鍵の配信を随時可能としている。すなわち図１において、例えば交換機ＳＷ２が呼発生時に相手先情報を中央管理制御装置２０に送信する。

【００３５】これに対し、中央管理制御装置２０ではデータベースを検索して相手先公開鍵と共通鍵情報を交換機ＳＷ２に送る。交換機ＳＷ２は、相手先公開鍵で共通鍵情報を暗号化して相手先の交換機ＳＷ４に送る。交換機ＳＷ４では、自己の公開鍵を用いて復号化することにより共通鍵を入手できる。

【００３６】したがって、交換機ＳＷ２と交換機ＳＷ４の間で共通鍵を用いてメッセージ情報を暗号化して送受することが可能となる。

【００３７】このように、本発明では、鍵の管理、運用を一元化して実施するセンター局と複数の交換機を個別に接続することにより、暗号化のための鍵の配信を随時可能とする。したがって、これまで個別に実施していた鍵管理の一元化を実施可能としたばかりでなく、必要により鍵の変更を行い、また、変更した内容を関連する装置に対して配信することが可能である。これにより、ネットワーク全体の融通性，拡張性を高めることが可能となる。

【００３８】さらに、回線秘匿方式に比較し、各呼単位に暗号化を実施することによりネットワークに近い場所で秘匿通信が実現可能となり、盗聴及び改竄が容易ではなくなる。また、交換機とそれに接続される加入者は、プライベートネットワークにおいては、同一事業所内であり基本的には交換機間で秘匿通信が必要である。

【００３９】図２は、センター局にある中央管理制御装置２０に設けられるデータベースを説明する図である。中央管理制御装置２０としてデータベース２０１に基づく鍵管理、変更機能２００を有する。データベース２０１は、複数の交換機Ａ～Ｘのそれぞれに対し公開鍵と秘密鍵が登録されている。公開鍵は送信データを暗号化するために用いられ自交換機以外の他の交換機に公開される鍵である。

【００４０】一方、秘密鍵は、公開鍵で暗号化され、他交換機から自交換機に送られた送信データを復号するために用いられる鍵である。図２において、更にデータベース２０２にはセンター局に与えられた公開鍵と秘密鍵が登録される。この公開鍵と秘密鍵は中央管理制御装置２０を有するセンター局と各交換機間で情報の送受を行なう時に用いられる。

【００４１】図３は、鍵の配布手順を説明する図である。図３において、ネットワークを構成する複数の交換機の内、交換機１０に収容される加入者から交換機１１に収容される加入者に対する呼が発生したと想定する。

【００４２】発信者側から呼が生起すると、交換機１０は秘匿通信を行なう通信モードに移行する（自動秘匿モード）。発信者側から発信番号の前に秘匿サービスに対応する個別番号を付けて発信することにより、秘匿動作モードに移行することも可能である（個別秘匿モード）。

【００４３】後者の場合は、交換機１０が個別番号（秘匿サービスの特定番号）をダイヤル情報より認識し秘匿サービスに移行する。

【００４４】図３において、秘匿サービスモードに移行した交換機１０は相手先ダイヤル番号と自交換機の利用者番号を、あらかじめネットワーク内に公開されている中央監視制御装置２０の公開鍵２０２を用いて暗号化する。これをＮｏ．７共通線信号ネットワーク２１を通して中央監視制御装置２０に送信する（ステップＳ１）。

【００４５】中央監視制御装置２０では、中央監視制御

装置２０の秘密鍵２０２により交換機１０から送られた暗号データを復号する。これにより、相手先ダイヤル番号と交換機１０の利用者番号を認識する。

【００４６】ここで、中央監視制御装置２０は、認識した相手先ダイヤル番号に基づきデータベース２０１を検索して相手先ダイヤル番号の属する（呼の送出先加入者を収容している）交換機１１の公開鍵（例えば、＊＊＊ｂ：２０１参照）を求める。中央監視制御装置２０は、更に求められた交換機１１の公開鍵及び、交換機１０，１１間で用いる共通鍵を交換機１０の公開鍵で暗号化して送信する（ステップＳ２）。

【００４７】交換機１０は、中央監視制御装置２０から送られた暗号化データを自交換機の秘密鍵で復号する。これにより交換機１０は、交換機１１の公開鍵と共通鍵を認識することが可能である。交換機１０は、更に復号化された共通鍵を交換機１１の公開鍵で暗号化して交換機１１に送信する。

【００４８】図４は、交換機１０における上記処理の流れを更に説明する図である。交換機１０は、加入者端末ＤＴから呼を上げる際に相手先ダイヤル番号とともに、秘匿サービス要求を交換機１０に対して送出する（ステップＳ１１）。この秘匿サービス要求は交換機１０の呼制御スイッチ部１１０で検知される（ステップＳ１２）。

【００４９】次いで、制御部１１１で呼の管理、相手先番号の抽出、加入者の秘匿サービス適用可否判断及び、センター局との対話データの作成等を制御部１１１で実行する（ステップＳ１３）。制御部１１１で作成された対話データがインタフェース１１２を通して、共通信号線網２１を介して中央管理制御装置２０に送られる（ステップＳ１４）。

【００５０】中央管理制御装置２０では先に説明したように図示しない加入者データから当該端末に秘匿サービスの適用が可か否かの判断を行なう。さらに、先に説明したように、データベース２１０（図２参照）に基づき鍵管理、検索、適用形態選択等の機能を行なう（ステップＳ１５）。

【００５１】さらに、交換機１０において、制御部１１１は中央管理制御装置２０に対し、暗号鍵の更新等を指示する。また、呼制御スイッチ部１１０に対し接続命令及び、秘匿開始命令を指示する（ステップＳ１６）。呼制御スイッチ部１１０は、秘匿開始命令を指示されると、暗号化部１００に対し送信情報の接続を行なう（ステップＳ１７）。

【００５２】暗号化部１００は、呼制御スイッチ部１１０により接続される送信情報を公開鍵により暗号化し、また暗号化された情報を秘密鍵により復号する復号化機能を有する。

【００５３】図３に戻り説明すると、一方、交換機１１では、受信した暗号化情報を自交換機の秘密鍵で復号化する。これにより、交換機１１において共通鍵を認識することができる。

【００５４】この時点で、生起した呼に対して端末を収容する交換機１０，１１（実際はそれぞれの交換機に備えられる暗号化部１００の間で、秘匿通信のための共通鍵の共有化が実現される。次いで、交換機１１の暗号化部１００において、共通鍵が準備された時点で交換機１０の暗号化部１００に対して返信を行なう。

【００５５】この間、交換機１０、１１に収容される端末側に対して、それぞれ秘匿処理の準備中であるアナウンスあるいは、特殊信号等を挿入することも可能である。それぞれの交換機の暗号化部間で同期が取れた時点でメッセージの秘匿通信を開始する。

【００５６】交換機１０の暗号化部においては、交換機１１の暗号化部との間で共有化した共通鍵をベースとして、例えば､DES, Triple DES等の暗号化方式を用いる暗号器により暗号化を行ない送信する。

【００５７】交換機１１の暗号化部１００では、受信した暗号文を共通鍵を用いて交換機１０の暗合化部１００の暗号化処理と逆手順により復号化を行なう。さらに、交換機１１に収容される端末側に対して復号されたメッセージを送信する。交換機１１の端末側からのメッセージは、前記内容を交換機１１からの逆手順で処理する。

【００５８】図５に暗号化部１００を付帯した交換機の機能ブロックを主体としてシステムの全体構成例を、図６に暗号化部１００の実施例ブロック図を示す。図５において、交換機の機能ブロックは、複数の交換機に共通であるので、交換機１０を例として説明する。

【００５９】交換機１０は、交換機１０に収容される端末ＤＴがアナログ端末又は、デジタル端末に区別されて、それぞれ接続されるアナログ加入者回路１１４、デジデジタル加入者回路１１５を有する。

【００６０】また、交換機１０は、呼制御スイッチ部１１０としてスイッチ１１０ａと、信号処理系１１０ｂを有する。さらに、回線交換網２２とのインタフェース機能を有するトランク１１３を有する。交換処理系１１１は、中央処理回路１２０、情報トランスレータ１２１及び、共通信号線網２１と接続される共通線信号処理回路１２２を有する。

【００６１】情報トランスレータ１２１を参照しながら、交換処理系１１１の中央処理回路１２０により全体制御が行なわれる。中央処理回路１２０により、共通線信号処理回路１２２がインタフェースとなり、共通線信号網２１に繋がる機器と制御信号の送受が行なわれる。

【００６２】信号処理系１１０ｂの監視回路１１３は、回線交換網２２に繋がるトランク１１３の出力状態を監視する。スイッチ制御部１３２は、中央処理回路１２０の制御に基づきスイッチ１１０ａの方路選択を制御する。

【００６３】Ｄチャネル制御回路１３０は、デジタル加

入者回路１１５を監視し、端末ＤＴのＤチャネルの状態を判断する。監視回路１３１は、アナログ加入者回路１１４の状態から呼の発生を監視する。そして、呼の発生を検知するとＤチャネル制御回路１３０及び、監視回路１３１は、接続先ダイヤル番号を中央処理回路１２０に通知する。

【００６４】中央処理回路１２０は、図６において後に説明するように、暗号化部１００により、中央管理制御装置２０の公開鍵を用いて接続先ダイヤル番号と自交換機番号を暗号化し、これを共通線信号処理回路１２２を通して共通線信号ネットワーク２１を介して中央管理制御装置２０に送る。

【００６５】中央処理回路１２０は、中央管理制御装置２０から共通鍵を通知されるとスイッチ制御回路１３２を制御して、スイッチ１１０ａの方路選択を行なう。暗号化部１００で共通鍵を用いて暗号化された通話情報は、選択されたスイッチ１１０ａの方路を経由しトランク１１３によりに回線交換網２２に送出される。

【００６６】ここで、アナログ加入者回路１１４及び、デジタル加入者回路１１５の出力を暗号化処理し、反対にトランク１１３の出力を復号化する暗号化部１００の実施例を図６により説明する。

【００６７】図６に示す暗号化部１００において、端末側インタフェース部１４３は、端末側インタフェース回路１４３ａと多重化／多重分離回路１４３ｂを有して構成される。そして、アナログ加入者回路１１４及び、デジタル加入者回路１１５との間でスイッチ１１０ａを通してデータの送受をインタフェースする機能を有する。

【００６８】一方、伝送路側インタフェース部１４４は、伝送路側インタフェース回路１４４ａと多重化／多重分離回路１４４ｂを有して構成される。そして、トランク１１３との間でスイッチ１１０ａを通してデータの送受をインタフェースする機能を有する。

【００６９】入出力部１４５は、交換機１０における交換処理系１１１の中央処理回路１２０と制御部１４２ｃとの間のインタフェース機能を有する。暗号化部１００は、鍵管理部１４１に中央管理制御装置２０の公開鍵ｃと自交換機（ここでは交換機１０である）の秘密鍵aを常時保持する。この公開鍵ｃと秘密鍵ａを用いて、先に図１～図３により説明したようにセンター局の中央管理制御装置２０から呼単位に相手局交換機（交換機１１とする）の公開鍵ｂと主信号（通話情報等）の暗号化／復号化を行なうための共通鍵（ａ－ｂ）を受信する。

【００７０】発信者側から呼が生起すると交換機１０は、秘匿通信を行なう通信モードに移行する。発信者側から意識的に秘匿サービスに個別番号を設け、発信番号の前に個別番号を付け発信することによる動作も可能である。

【００７１】この場合交換機１０は、個別番号（秘匿サービスの特定番号）をダイヤル情報より検知してＤチャネル制御回路１３０及び、監視回路１３１（図５参照）において秘匿サービス要求があることを認識する。これにより交換機１０の中央処理回路１２０の制御により秘匿サービスに移行する。

【００７２】秘匿モードに移行すると、暗号化部１００の制御部１４２と交換機１０の中央処理回路１２０により制御が開始される。秘匿サービスモードに移行した交換機１０は、中央処理回路１２０からの秘匿サービスモード通知に基づき、制御部１４２のセンター局鍵送受制御回路１４２ｃにより相手先番号と利用者番号をセンター局の公開鍵ｃにより暗号化する。次いで、中央処理回路１２０により、暗号化された相手先番号と利用者番号を共通信号線ネットワーク２１を通して中央管理制御装置２０に送信する。

【００７３】中央管理制御装置２０では、交換機１０から送られた暗号データを秘密鍵ｃで復号化し、相手先番号と利用者番号を認識する。そして、復号化された相手先番号と利用者番号を基にデータベース２０１（図２参照）を検索する。この検索により相手先の端末が接続される交換機（例えば、交換機１１）の公開鍵ｂが求められる。さらに、中央管理制御装置２０は、交換機１０と交換機１１間で実際に通信されるメッセージを暗号化するための共通鍵（ａ－ｂ）を生成する。

【００７４】このように生成された共通鍵（ａ－ｂ）と、この共通鍵（ａ－ｂ）を交換機１１と通信するのための交換機１１の公開鍵ｂを、交換機１０の公開鍵aにより暗号化して中央管理制御装置２０から交換機１０に送信する。

【００７５】交換機１０では、中央管理制御装置２０より受信した暗号化データを暗号化部１００のセンター鍵送受制御回路１４２ｃで交換機１０の秘密鍵ａを用いて復号する。これにより交換機１１の公開鍵ｂとメッセージを暗号化する際に使用する共通鍵（ａ－ｂ）が求められる。

【００７６】交換機１０は、中央制御回路１２０の制御によりスイッチ制御回路を通してスイッチの方路選択を行なって、相手先ダイヤル番号に従う接続処理を行なう。一方、交換機１１においては、接続処理が行なわれると秘匿通信モードに移行する。この時点で交換機１０の暗号化部１００と交換機１１の暗号化部が共通信号線ネットワーク２１を通して接続される。

【００７７】接続された時点で、交換機１０の暗号化部１００の共通鍵制御部１４２ａにより中央管理制御装置２０から指示された交換機１１の公開鍵ｂで、共通鍵（ａ－ｂ）を暗号化する。そして、暗号処理部１４０の共通鍵送受信部１４０ａにより交換機１１の暗号化部に送信する。

【００７８】交換機１１の暗号化部では、受信したデータを秘密鍵ｂで復号化し、共通鍵（ａ－ｂ）を再生する。この時点で、生起した呼に対して、端末を収容する

交換機間（実際はそれぞれの交換機の暗号化部）で、秘匿通信の鍵（共通鍵ａ－ｂ）の共有化が実現される。

【００７９】このとき、交換機１１の暗号化部において、共通鍵（ａ－ｂ）が準備された時点で、交換機１０の暗号化部１００に対して返信を行ない確認する。

【００８０】この間、端末側に対しては、秘匿処理の準備中であるアナウンス等を挿入することも可能である。この際、制御部１４２の中央制御回路１４２ａと交換処理系１１１の中央処理回路１２０との間で状況確認を実施することとなる。

【００８１】次いで、それぞれの交換機１０，１１の暗号化部間で同期が取れた時点でメッセージの秘匿通信を開始する。交換機１０の暗号処理部１４０においては、交換機１１の暗合化部との間で共有化した共通鍵（ａ－ｂ）を暗号化部１００の鍵管理部１４１より暗号処理部１４０に対して送信する。暗号処理部１４０の暗合器１４０ｂは、前記共通鍵（ａ－ｂ）を用いて、例えば、DES, TripleＤＥＳ等の暗号化方式により暗合化を行なう。この暗号化されたメッセージは、伝送路インタフェース部１４４を通して回線交換網２２に送信される。

【００８２】交換機１１の対応する暗号化部（暗号処理部の復号器）では、受信した暗合文を共通鍵（ａ－ｂ）を用い、交換機１０側の暗合器１４０ｂと逆の手順により復号器１４０ｃにより復号化を行なう。次いで、端末側に対して復号化したメッセージを送信する。交換機１１の端末側からのメッセージは、交換機１０と同様に共通鍵（ａ－ｂ）を用い暗号化して、交換機１０側に送信する。

【００８３】呼が完了した時点で、暗号化部１００の制御部１４２は、鍵管理部１４１に対して公開鍵ｂ及び共通鍵（ａ－ｂ）を破棄するように指示し、これらの鍵は破棄される。

【００８４】さらに、センター局の中央管理制御装置２０の公開鍵ｃと自交換機の秘密鍵aも、中央管理制御装置２０との上記送受手順と同様にして通信を行ない、鍵管理部１４１のデータベースを変更することが可能である。このため、鍵管理が容易となるばかりでなく、秘匿システムとして強化が可能となる。

【００８５】図７は、本発明の別の実施例である。秘匿の精度を高めるためには情報発信部に近いところにおいて、暗号化、復号化を行なうことが望ましい。かかる場合、図７に示すように、個々の端末３００に秘匿装置を設けるようにすることで可能である。

【００８６】すなわち、図７では簡略して示されているが、図６で説明した暗号化部１００野機能の一部を個別端末３００に置くことが可能である。図７において、端末３００は、制御部３０１により暗号化／復号化の機能が制御される。

【００８７】自端末の公開鍵レジスタ３０３、公開鍵に対応する秘密鍵レジスタ３０２を有する。そして、センター局の中央管理制御装置２０に送られる暗号化データを秘密鍵３０２で復号化することにより共通鍵３０４が再生される。

【００８８】したがって、再生された共通鍵３０４を用い、相手先端末に向けたメッセージを暗号器３０５で暗号化して、端末３００の接続される交換機１０に送出することがが可能である。

【００８９】図７の実施例の場合、交換機１０の暗号化部１００の機能として、中央管理制御装置２０に対し、相手先端末のダイヤル情報及び、交換機１０の利用者番号を暗号化して通知する機能部分を有する様に構成すればよく、暗号化部１００の構成が簡易となる。

【００９０】

【発明の効果】以上実施例に従い説明したように、本発明により加入者側において鍵管理を実施することなく、各呼単位に秘匿通信を実施することが可能となる。秘匿通信の度に鍵を変更（強制的）ができる。センター局が鍵管理を一元的に実施しているため、保守，機密性も向上可能となる。さらに、センター局とネットワークを構成する複数の交換機間のデータを送受する鍵については、共通線ネットワークにより通信路を確保しているため、ネットワーク内で随時鍵を変更することも可能である。

【００９１】したがって、本発明によりプライベート・ネットワークにおいて、各ユーザが意識することなく、秘匿ネットワークを構築することが可能である。セキュリティを強化することができるばかりでなく、システムを変更することなく個別に特定ユーザに対して設定することが可能となる。

【００９２】さらに、中央管理制御装置により一元的に鍵管理を実施することが可能となるため、管理対象を限定することができるばかりでなく、それぞれの鍵を随時又は必要により変更することが可能となる。これによりシステムとしてのセキュリティを強化することができる。また、システムを拡張する場合においても、中央管理制御装置から指示することが可能である。

【００９３】さらにまた、秘匿装置の暗号器（秘匿方式）の組合せも呼単位に変更することができる。

【図面の簡単な説明】

【図１】本発明に従うネットワークシステムにおける秘匿サービス機能の原理を説明する図である。

【図２】センター局にある中央管理制御装置２２に設けられるデータベースを説明する図である。

【図３】鍵の配布手順を説明する図である。

【図４】交換機１０における上記処理の流れを更に説明する図である。

【図５】暗号化部１００を付帯した交換機の機能ブロックを主体としてシステムの全体構成例を示す図である。

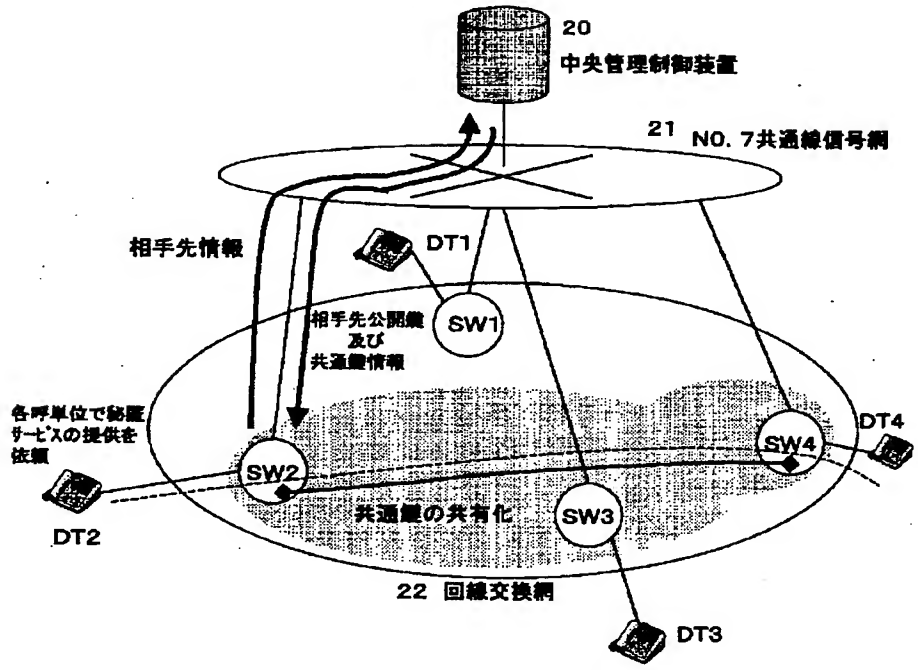
【図６】暗号化部１００の実施例ブロック図である。

【図７】本発明の別の実施例である。

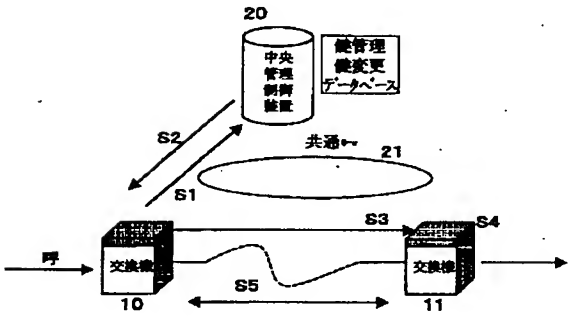
【図８】秘匿通信の概略を説明する図である。
【図９】端末暗号方式を説明する図である。
【図１０】回線暗号方式を説明する図である。
【図１１】従来の秘匿システムの一例を示す図である。
【符号の説明】

２０　中央管理制御装置
２１　共通信号線ネットワーク
２２　公衆回線網
１０、１１　交換機
２０１　データベース

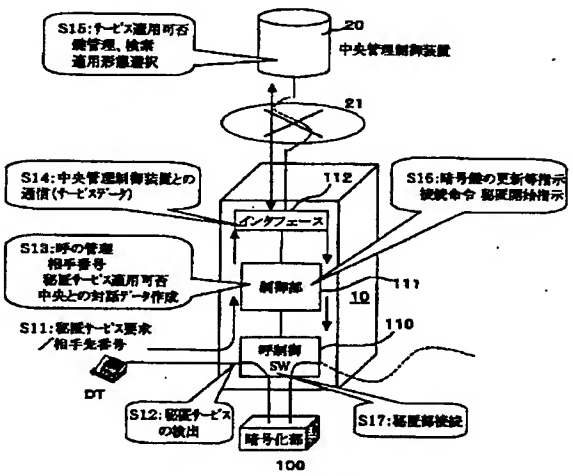
【図１】



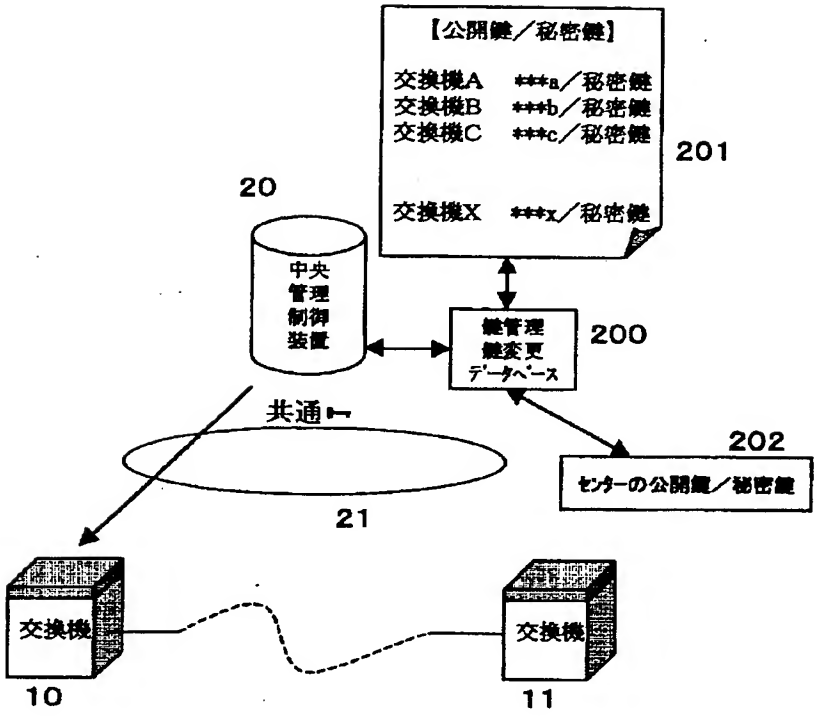
【図３】



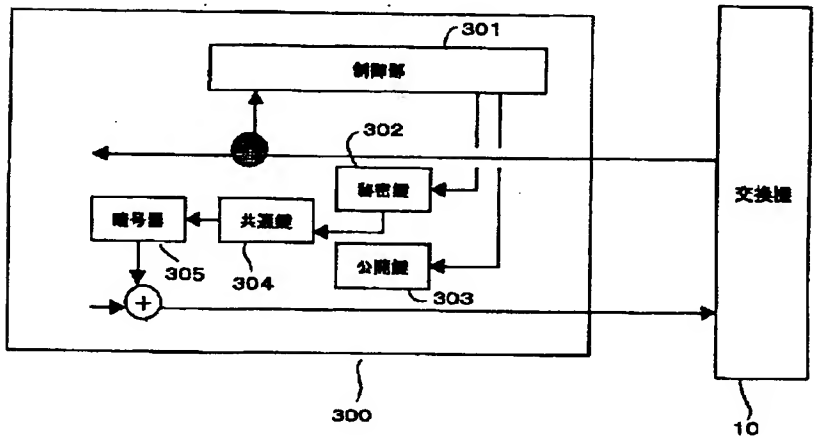
【図４】



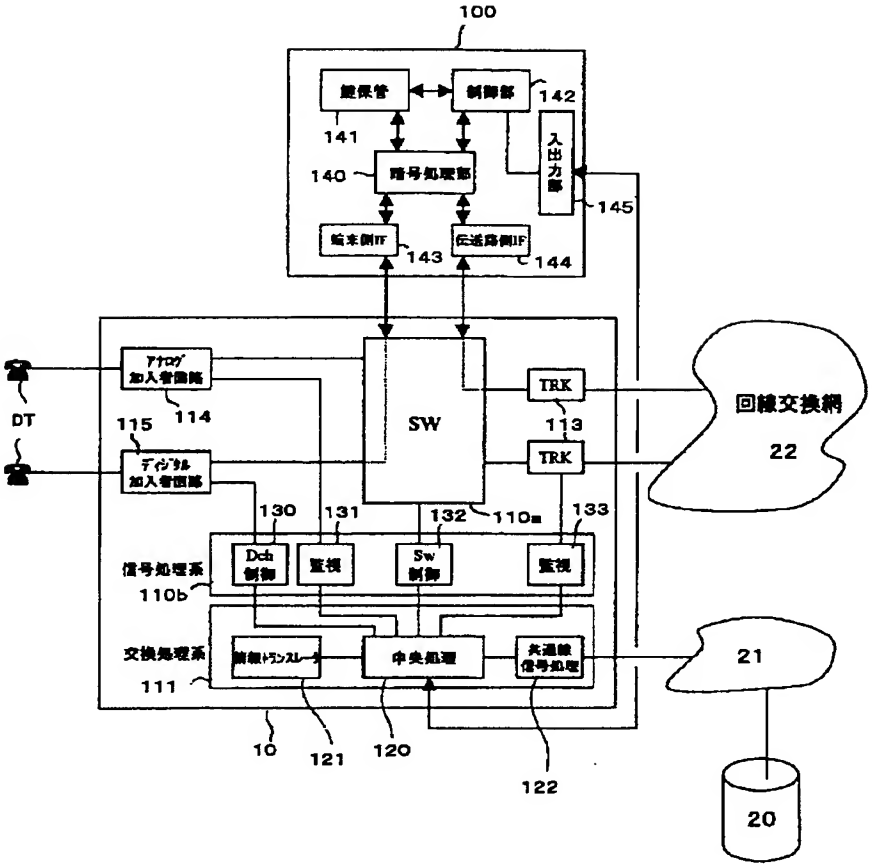
【図２】


【公開鍵／秘密鍵】
交換機A　***a／秘密鍵
交換機B　***b／秘密鍵
交換機C　***c／秘密鍵
交換機X　***x／秘密鍵
201
20
中央管理制御装置
鍵管理鍵変更データベース
200
共通
202
センターの公開鍵／秘密鍵
21
交換機
交換機
10
11

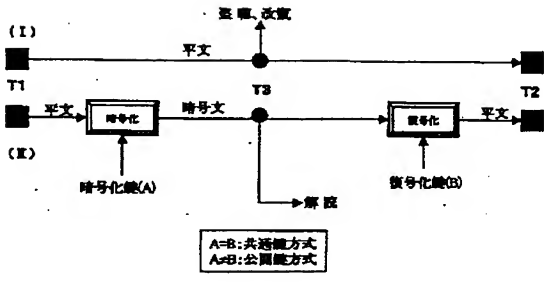
【図７】


301
制御部
302
秘密鍵
暗号器
共通鍵
公開鍵
305
304
303
交換機
300
10

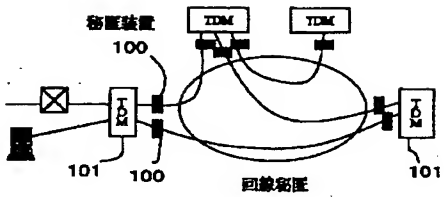
【図５】


100
鍵保管
制御部
142
141
入出力部
140
暗号処理部
145
端末側IF
143
伝送路側IF
144
アナログ加入者回路
DT
115
114
SW
TRK
113
回線交換網
22
ディジタル加入者回路
TRK
130
131
132
110a
133
信号処理系
Dch制御
監視
Sw制御
監視
110b
交換処理系
制御トランスレータ
中央処理
共通線信号処理
111
21
10
121
120
122
20

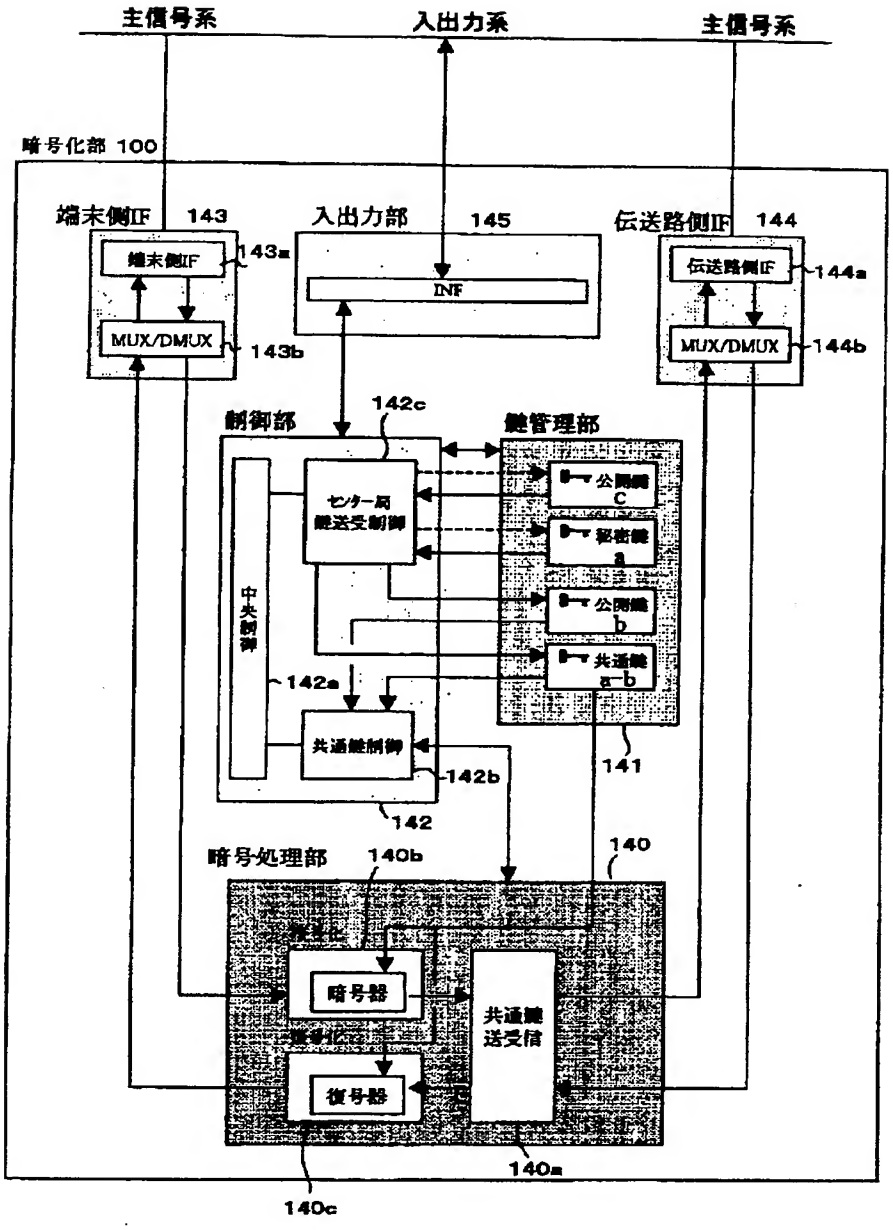
【図８】


(I)
平文
T1
T3
T2
平文
暗号化
暗号文
復号化
平文
(II)
暗号化鍵(A)
復号化鍵(B)
A=B:共通鍵方式
A≠B:公開鍵方式

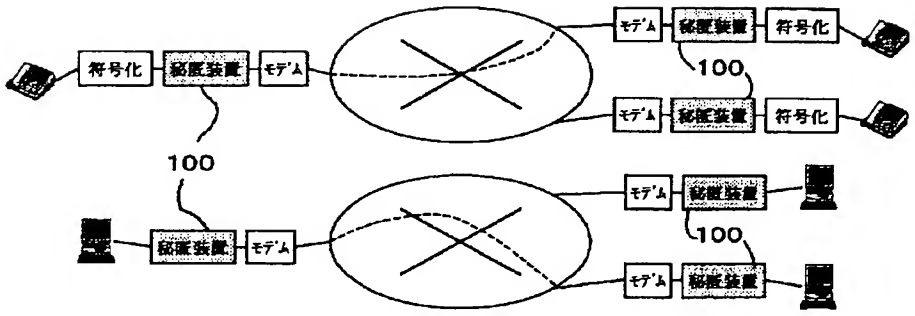
【図１０】


TDM
TDM
100
101
100
回線収容
101

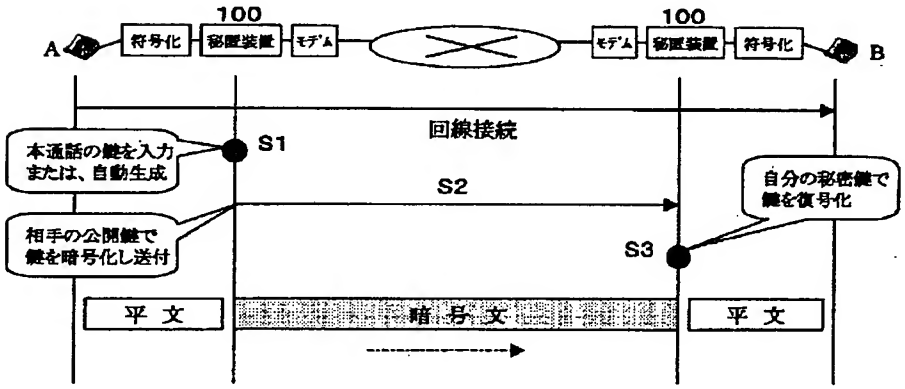
【図６】


主信号系
入出力系
主信号系
暗号化部 100
端末側IF 143
143a
端末側IF
MUX/DMUX
143b
入出力部 145
INF
伝送路側IF 144
144a
伝送路側IF
MUX/DMUX
144b
142c
制御部
鍵管理部
センター局
鍵送受制御
中央制御
公開鍵
C
秘密鍵
a
公開鍵
b
共通鍵
a-b
142a
共通鍵制御
142b
142
141
暗号処理部
140b
140
暗号化
暗号器
共通鍵
送受信
復号化
復号器
140a
140c

【図９】



【図１１】



フロントページの続き

(51) Int. Cl.⁷	識別記号	FI		ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｍ　7/00		Ｈ０４Ｌ　9/00	６０１Ａ	
			６０１Ｅ	
		11/20	Ｂ	

Ｆターム（参考）　5B089 GA01 GA34 HA01 JA00 JB22
KA17 KC57 KH30
5J104 AA16 AA34 BA01 EA01 EA06
EA19 JA03 MA06 NA02 NA03
NA05 PA07
5K024 AA00 DD05 GG08
5K030 GA15 HA01 HC01 HD05 KA07
LD17
5K051 AA00 CC08 DD01 FF01 GG01
GG13 HH04 HH15 JJ02